#6

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES	Docket Number (Optional) 42390P10855

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

January 16, 2004

Signature Marilyn Bass

Typed or printed name Marilyn Bass

In re Application of
Michael S. Ripley, et al.

Application Number	Filed
09/823,423	03/29/2001

For
METHOD AND SYSTEM FOR PROVIDING BUS

Art Unit	Examiner
2131	Lee, Chi Chung

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 1.17(b)) $330.00

☐ Applicant claims small entity status under 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: _____

☒ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of the fee transmittal.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 02-2666. I have enclosed a duplicate copy of the fee transmittal.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2039.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.

☐ attorney or agent acting under 37 CFR 1.34(a). Registration number if acting under 37 CFR 1.34(a) _____.

Signature

Walter T. Kim, Reg. No. 42,731
Typed or printed name

01/16/04
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

Based on PTO/SB/31 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 09/11/2003.
SEND TO: Mail Stop Appeal, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

01/21/2004 MGEBREM1 00000167 09823423

01 FC:1401 330.00 OP

AF/2700

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/823,423
Filing Date	March 29, 2001
First Named Inventor	Michael S. Ripley
Art Unit	2131
Examiner Name	Lee, Chi Chung
Total Number of Pages in This Submission	4
Attorney Docket Number	42390P10855

ENCLOSURES *(check all that apply)*

- [X] Fee Transmittal Form
  - [X] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*

Return receipt postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Walter T. Kim, Reg. No. 42,731 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	Walter T. Kim
Date	January 16, 2004

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	Marilyn Bass		
Signature	Marilyn Bass	Date	January 16, 2004

Based on PTO/SB/21 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wtr) 09/11/2003.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 330.00

Complete if Known	
Application Number	09/823,423
Filing Date	March 29, 2001
First Named Inventor	Michael S. Ripley
Examiner Name	Lee, Chi Chung
Group/Art Unit	2131
Attorney Docket No.	42390P10855

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims		- 26** =		X	=
Independent Claims		- 3 =		X	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920 *	1804	920 *	Requesting publication of SIR prior to Examiner action	
1805	1,840 *	1805	1,840 *	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	1,210	2255	605	Extension for reply within fifth month	
1404	330	2401	165	Notice of Appeal	330.00
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 330.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Walter T. Kim	Registration No. (Attorney/Agent)	42,731	Telephone	(310) 207-3800
Signature	Walter T. Kim			Date	01/16/04

Based on PTO/SB/17 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 08/11/2003.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Baron, Gilberto

PTO 03-4964

Japanese Article

DVD COPYRIGHT PROTECTION SYSTEM

[DVD Chosakuken Hogo Shisutemu]

Natsume Matsuzaki*1, Makoto Tatebayashi*1,

Hideshi Ishihara*2, and Yoshihisa Fukushima*2

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C. August 2003

Translated by: Schreiber Translations, Inc.

Translated Title	:	DVD COPYRIGHT PROTECTION SYSTEM (subtitled: DVD Content Scramble System)
Foreign Title	:	DVD Chosakuken Hogo Shisutemu
Authors	:	Natsume Matsuzaki*1, Makoto Tatebayashi*1, Hideshi Ishihara*2, and Yoshihisa Fukushima*2
Author Affiliation	:	*1: Multimedia Development Center; *2: Optical Disc Systems Development Center
Source	:	National Technical Report, Vol. 43, No. 3, June 1997, pp. 338-42

Abstract

The CSS (Content Scramble System), which is a DVD copyright protection system which takes advantage of encryption, has been developed. The present system is based on an encryption technology developed by the present company, and it has, based on debates at the DVD Consortium, been accorded with fundamental agreements among technical experts of the private electronic consumer product industry, motion picture industry, computer industry, etc. The objective of the present system is to prevent casual copying by a general user based on the use of a computer. The CSS is therefore founded on the following encryption technical rationales:

(1): Content encryption: Contents obtained as a result of MPEG compression are encrypted by using a three-layered key combination of a title key, a disc key, and a master key. The encrypted contents can only be decoded and played back by licensed DVD models that comply with the CSS standards.

(2): Bus authentication: A DVD-ROM drive and an MPEG decoder module within a PC system are mutually authenticated. An unauthorized copying via the PC bus is prevented.

1. Preface

[1] Numbers in the margin indicate pagination in the foreign text.

In accordance with the proliferated uses of digital copyrighted artifacts that abound in AV environments and PC environments in recent years, the copyright protection has become a critical issue. The copyright protection signifies the prevention of an unauthorized use of a copyrighted artifact without obtaining its author's consent, and a copy prevention technology which prevents an unauthorized recording of a digital copyrighted artifact from one medium to another is an essential mechanism for copyright protection.

The DVD meets the requisites for motion picture software package media in that it is /2
capable of recording high-quality animate images of at least 2 hours on a single disc. The DVD, however, is also classified as an AV/computer unified medium which can be used not only for DVD players but also in computer environments, and in contradistinction with extant digital media such as the DAT, MD, etc., it easily enables not only the copying of digitally recorded information by a general user who has access to a computer but also the quotation of a still image obtained by partially clipping an animate image and the dissemination of such data to external parties via a network.

It is against such a backdrop that the motion picture industry has come to urge, as a requisite for providing motion picture software as DVD contents, a "copyright protection measure which uses an encryption technology" far more strict than those for extant digital media for the purpose of preventing

unauthorized copying by a general user based on a computer. Debates were exchanged, in response to such a demand, mainly among three DVD-related industries [i.e., private electronic consumer product industry (inclusive of the present company), motion picture and music industries, and computer industry which uses DVDs as peripheral media), and a decision was made at a technical consortium to develop a technology agreed upon with regard to the DVD copyright protection.

The copyright protection system which is being currently orchestrated for DCD playback machines is referred to as the "Content Scramble System" (CSS), and these three industries have basically agreed upon it. A copyright holder can guarantee copyright protection of contents based on the adoption of the CSS technology, whereas playback machine manufacturers, too, can play back encrypted discs based on the adoption of the CSS technology. The present company has developed an encryption technology which provides the foundation of said CSS technology.

In the present article, views on the copyright protection of the CSS and the orchestrated encryption technology will be discussed.

2. Summary of the CSS system

2.1. Objective of CSS

The objective of the DVD copyright protection system CSS (Content Scramble System) is the prevention of casual copying, namely the endowment of a sufficient level of protection capacity

for preventing unauthorized copying by a general user via a household appliance. The "casual copying" signifies unauthorized copying procedures such as simple copying on a hard disc, etc. based on a general user's attempt to reconnect an AV machine connection cord or to operate a keyboard in a computer environment. The following two encryption formats are orchestrated for the CSS in order to achieve the aforementioned objective:

(1): Content encryption

Contents on a disc are encrypted. Decoding technologies and keys necessary for playing back the encrypted contents are managed and disseminated by a neutral organization.

(2): Bus authentication

Mutual mechanical authentications are exchanged between a DVD-ROM drive and an MPEG decoder module connected via a computer bus. Based on this setup, unauthorized copying of a copyrighted artifact onto a hard disc, etc. connected to the computer bus and the playback of an unauthorized copy from the decoder module can be prevented.

In addition to these encryption technologies, the following features are assigned to DVD-related products for the purpose of preventing casual copying.

* Analog video image output

The DVD player or DVD-ROM drive does not, without administering an anti-copying measure, emit an analog output of an

originally scrambled digital video image after it has become descrambled.

* Digital video image output

The DVD player or DVD-ROM drive does not emit a digital output of the descrambling result of an originally scrambled digital video image.

Incidentally, the DVD copyright protection system is not intended to prevent the duplications of pirated DVD versions or unauthorized copying based on hardware (e.g., player, etc.) modification. Special apparatuses, expertise, skills, and costs are required for committing these unauthorized acts, and therefore, they are not considered as unauthorized acts of general users.

2.2. Constitution of the system

The overall constitution of the DVD copyright protection system is shown in Figure 1. The following are executed by the present system.

(1): In a disc preparation embodiment, the contents are initially MPEG-compressed and then encrypted by means of content encryption for preparing a disc.

(2): The prepared disc can be played back in both AV environments and computer environments.

(3): In a case where [said disc is] used in AV environments, a content decoding routine orchestrated for a normal DVD player is

executed, and after the obtained results have been MPEG-decoded and then D/A-converted, analog AV signals are played back.

(4): In a case where [the same is] used in computer environments, the DVD-ROM drive and MPEG decoder module authenticate one another via the computer bus (i.e., bus authentication). The content decoding key information is then encrypted based on a time-variable key which has come to be commonly shared, and subsequently, it is transmitted. The MPEG decoder module executes, following the bus authentication, a content decoding routine, and after the obtained results have been MPEG-decoded and then D/A-converted, analog AV data are played back.

2.3. Characteristics of the system

(1): Content encryption position: Video image and/or sound data obtained as a result of MPEG compression are subjected to the content encryption. In the playback mode, MPEG decoding is executed after content decryption. For this reason, no adverse effects are exerted on the MPEG compression ratio, image quality, etc. by the content encryption. /3

(2): Compatibility: Copyright protected DVDs are compatible not only with stand-alone players but also with PC systems, which are both household electronic appliances.

(3): Triple-layer key management: The content encryption involves a triple-layer key management scheme inclusive of a title key, a disc key, and a master key.

(4): Security: As has been mentioned earlier, the CSS prevents casual copying by general users. A higher level of security can be realized by using an unpublicized encryption algorithm.

3. Content encryption

3.1. Summary of content encryption

The contents on a DVD are encrypted by using triple-layer keys (i.e., title key, disc key, and master key), and only licensed DVD machines which comply with the CSS standards are capable of decoding and playing them back. The DVD machine that complies with the CSS standards may, for example, be endowed with a mechanism which prohibits a general user from copying digitally in a case where no digital information is being outputted in a decrypted state.

3.2. Encryption of three layers

The following three types of encryption keys are used in a hierarchical fashion for encrypting the contents.

(1): Title key

It is a key freely selected by a copyright holder (e.g., movie director) in manners specific to titles stored on the disc. The contents are scrambled by using this key.

(2): Disc key

It is a key freely selected by a copyright manager (e.g., movie company) in disc-specific fashions. The title key of (1) is encrypted by using this key.

(3): Master key

It is a key assigned to each descrambler manufacturer specializing in the decoding of the contents. The disc key of (2) is encrypted by using the master keys of the respective manufacturers.

3.3. Procedures for encrypting the contents

The procedures for encrypting the contents will be shown below with reference to Figure 2. Incidentally, the "CSS management organization" in the figure signifies a neutral organization that manages the CSS (which is currently in the process of being set up).

(1): Formulation of AV data

A content creator (= copyright holder) formulates contents and then decides whether or not to encrypt the contents.

(2): Decisions on the title key and disc key

In a case where the contents are encrypted, the copyright holder freely determines the title key. In a case where more than one encrypted titles are included in a disc, the copyright holder freely selects one disc key from among them.

(3): Scrambling of the contents

The AV contents obtained as a result of MPEG compression are scrambled by using the title key selected by the copyright holder. The contents are scrambled by the disc manufacturer.

(4): Encryption of the title key

The title key is encrypted by using the disc key selected by the copyright manager. The encrypted title key is stored in the sector header region on the disc which is inaccessible to users.

(5): Encryption of the disc key

The disc key is encrypted by using the master key and then converted into an encrypted disc key set. The master keys of the respective manufacturers are managed strictly in this conversion box. The encrypted disc key set obtained as a conversion result is stored in the lead-in region on /4
the disc which is inaccessible to users. The encryption of the disc key and the encryption of the title key are executed by the CSS management organization.

3.4. Procedures for decoding the contents

The procedures for decoding the contents on a DVD player will be shown below with reference to Figure 3. Incidentally, a hidden master key corresponding to the manufacturer licensed by the CSS is preliminarily built into the DVD player.

(1): The encrypted disc key set on the disc is decoded by using the internalized master key for ascertaining the disc key.

(2): The encrypted title key on the disc is decoded by the disc key ascertained above for ascertaining the title key.

(3): The scrambled AV data on the disc are descrambled by the title key ascertained above, and the obtained results are MPEG-decoded for playing back the original video image and sound.

3.5. Application embodiment for decoding the contents on the DVD player

A representative embodiment wherein a descrambling LSI which decodes the contents is integrated with the DVD player will be explained.

An approximate constitution of the DVD player is shown in Figure 4. The descrambling LSI, which is indicated by the hatched portion of the figure, is connected not only to a microcomputer bus which controls the entire player but also to an error correction LSI and an MPEG video decoder LSI.

The descrambling LSI receives, under the control of the controller microcomputer of the DVD player, the scrambled data decoded from the DVD via the error correction LSI and then descrambled said data. The descrambled AV data are transferred to the MPEG video decorder LSI orchestrated at the subsequent step, MPEG-decoded, and then played back.

The descrambling LSI is characterized by a specification which prohibits the decoding of the disc key and title key prevailing as intermediate content decoding results for the purpose of ensuring the security of the CSS technology.

4. Bus authentication

4.1. Outline of bus authentication

A DVD-ROM drive and an MPEG decoder module, which are connected via a computer bus (PC bus), mutually authenticate that they are both machines which comply with the CSS standards, and key information is encrypted and disseminated by using a time-variable key. This setup prevent unauthorized copying of a copyrighted artifact decoded from the DVD by the DVD-ROM drive onto a hard disc, etc. which are connected to the PC bus and which do not comply with the CSS standards. The decoder module that complies with the CSS standards, furthermore, prevents the playback of an unauthorized copy stored in the hard disc which does not comply with the CSS standards.

The procedures for transferring the data decoded from the DVD by the DVD-ROM drive of the PC system to the DVD-ROM drive and for playing them back will be explained below with reference to Figure 5.

(1): Bus authentication

The DVD-ROM drive executes the bus authentication via the DVD-ROM drive and PC /5
bus. In a case where the bus authentication fails, the transfer of data from the DVD-ROM drive to the MPEG decoder module is stopped.

(2): Secret transmission of key information by using the time-variable key

A secret time-variable key comes to be commonly shared by the DVD-ROM drive and MPEG decoder module as bus authentication results. The content encryption key information is secretly relayed to the MPEG decoder module by using this time-variable key.

(3): Content decoding

The bus authentication is followed by the decoding of the contents according to procedures identical to those of 3.4, based on which the AV data become played back.

4.2. Application embodiment for bus authentication and content decoding in PC environments

A representative embodiment wherein an LSI which executes the bus authentication and content decoding is integrated with a DVD-ROM drive and an MPEG decoder card in PC environments will be explained.

Approximate constitutions of the DVD-ROM drive and MPEG decoder card are shown in Figure 8. The authentication LSI in the drive hatched in the figure, which realizes the bus authentication, is connected to the bus of a microcomputer which controls the entire drive. The descrambling LSI on the decoder card, which is endowed with an authentication function, is mounted on a single chip for realizing both the bus authentication and content decoding. [Said descrambling LSI is] connected not only to a host CPU via a local bus of a PCI interface LSI on the

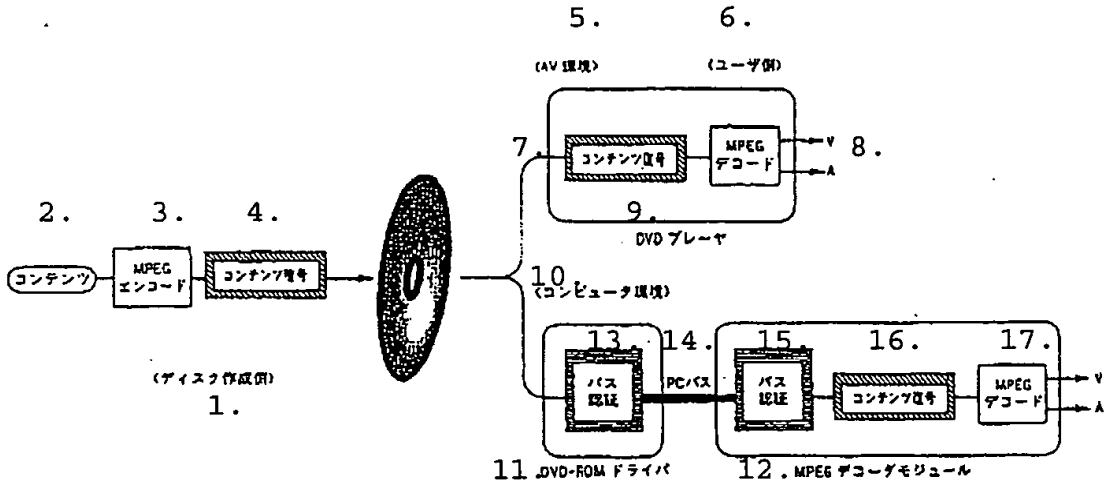
decoder card but also to a stream transfer port of the PCI interface LSI and MPEG decoder LSI.

The descrambling LSI endowed with an authentication function is characterized by a constitution which prohibits the decoding of data prevailing during the bus authentication and content decoding by an external party. Based also on a specification which prohibits the decoding of the disc key and title key prevailing as intermediate content decoding results, furthermore, the security of the CSS technology is ensured. Incidentally, in a case where measures that satisfy the foregoing requisites are administered with regard to the CSS security, the bus authentication and content decoding can be executed by PC software.

5. Conclusions

The objective and technical contents of the DVD copyright protection system CSS have been discussed above. The objective of the CSS is to prevent casual copying, and in this context, the CSS is endowed with a pair of encryption mechanisms, namely the encryption of contents and the bus authentication for preventing copying on a PC system bus.

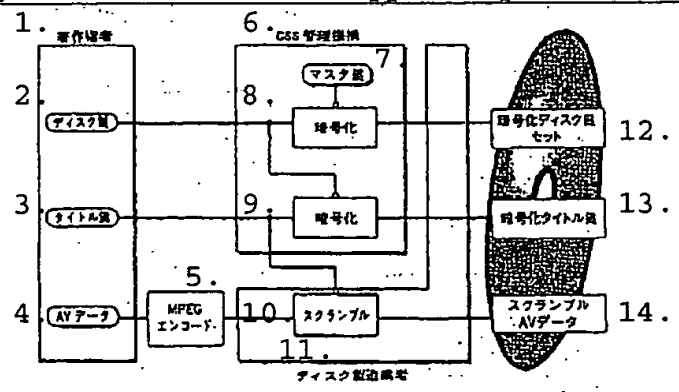
Figure 1: Overall constitution of DVD copyright protection system CSS



第1図 DVD著作権保護システム CSS (Content Scramble System) の全体構成 Fig. 1 Block diagram of CSS.

[(1): Disc preparation embodiment; (2): Contents; (3): MPEG encode; (4): Content encryption; (5): AV environment; (6): User side; (7): Content decoding; (8): MPEG decode; (9): DVD player; (10): Computer environment; (11): DVD-ROM driver; (12): MPEG decoder module; (13): Bus authentication; (14): PC bus; (15): Bus authentication; (16): Content decoding; (17): MPEG decode]

Figure 2: Content encryption procedures

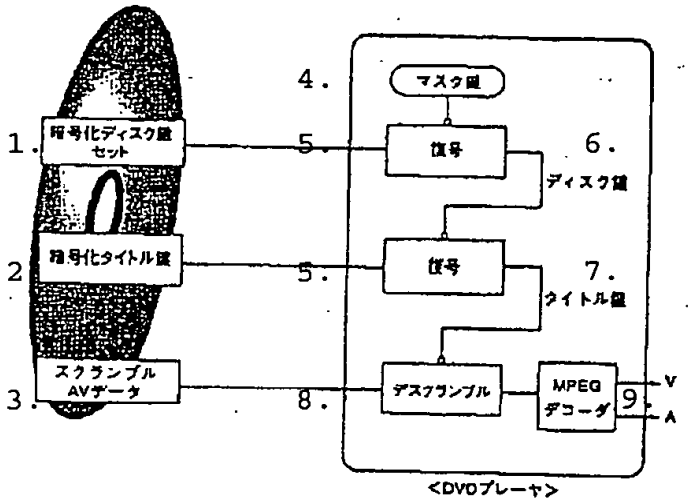


第2図 コンテンツ暗号の手順

Fig. 2 Content scramble hierarchy.

[(1): Copyright holder; (2): Disc key; (3): Title key; (4): AV data; (5): MPEG encode; (6): CSS management organization; (7): Master key; (8): Encryption; (9): Encryption; (10): Scramble; (11): Disc manufacturer; (12): Encrypted disc key set; (13): Encrypted title key; (14): Scrambled AV data]

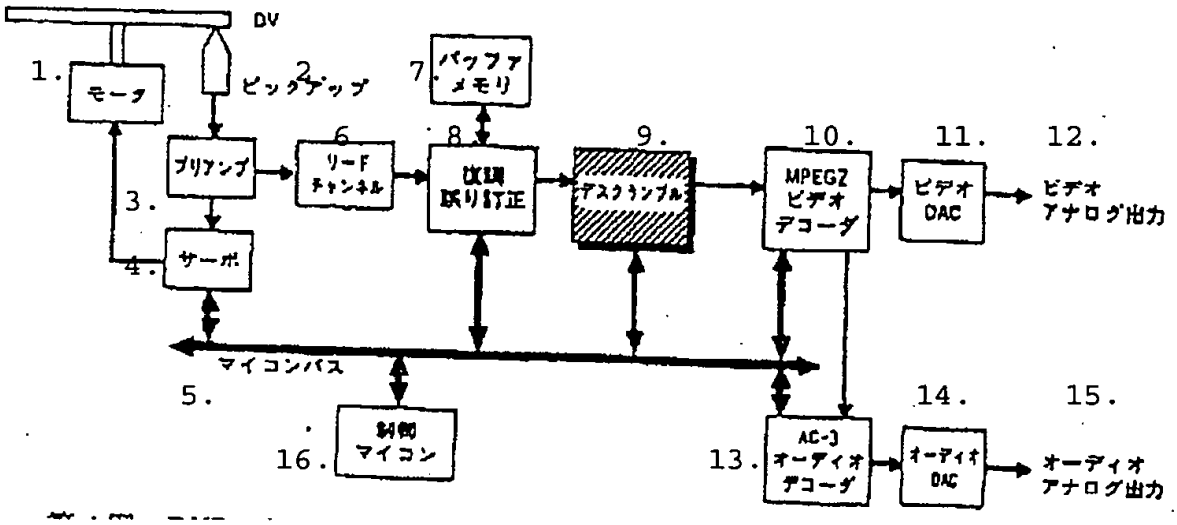
Figure 3: Decoding of contents by DVD player



第3図 DVDプレーヤにおけるコンテンツ復号
Fig. 3 Content descramble in DVD player.

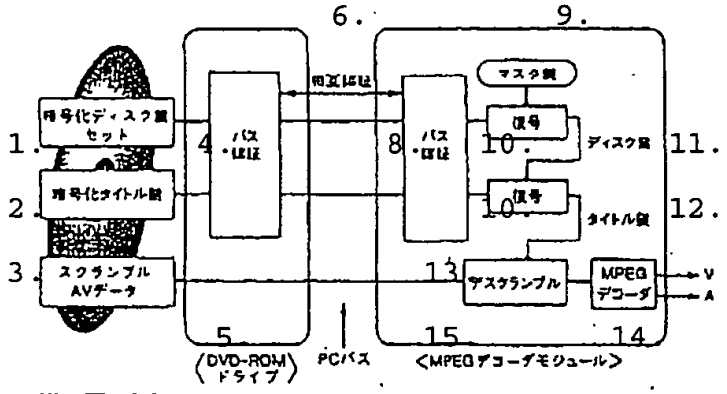
[(1): Encrypted disc key set; (2): Encrypted title key; (3): Scrambled AV data; (4): Master key; (5): Decoding; (6): Disc key; (7): Title key; (8): Descramble; (9): MPEG decoder; (10): DVD player]

Figure 4: Approximate constitution of DVD player



[(1): Motor; (2): Pickup; (3): Preamplifier; (4): Servo; (5): Microcomputer bus; (6): Lead channel; (7): Buffer memory; (8): Demodulation and error correction; (9): Descramble; (10): MPEG2 video decoder; (11): Video DAC; (12): Video analog output; (13): AC-3 audio decoder; (14): Audio DAC; (15): Audio analog output; (16): Controller microcomputer]

Figure 5: Bus authentication and content decoding in a PC system

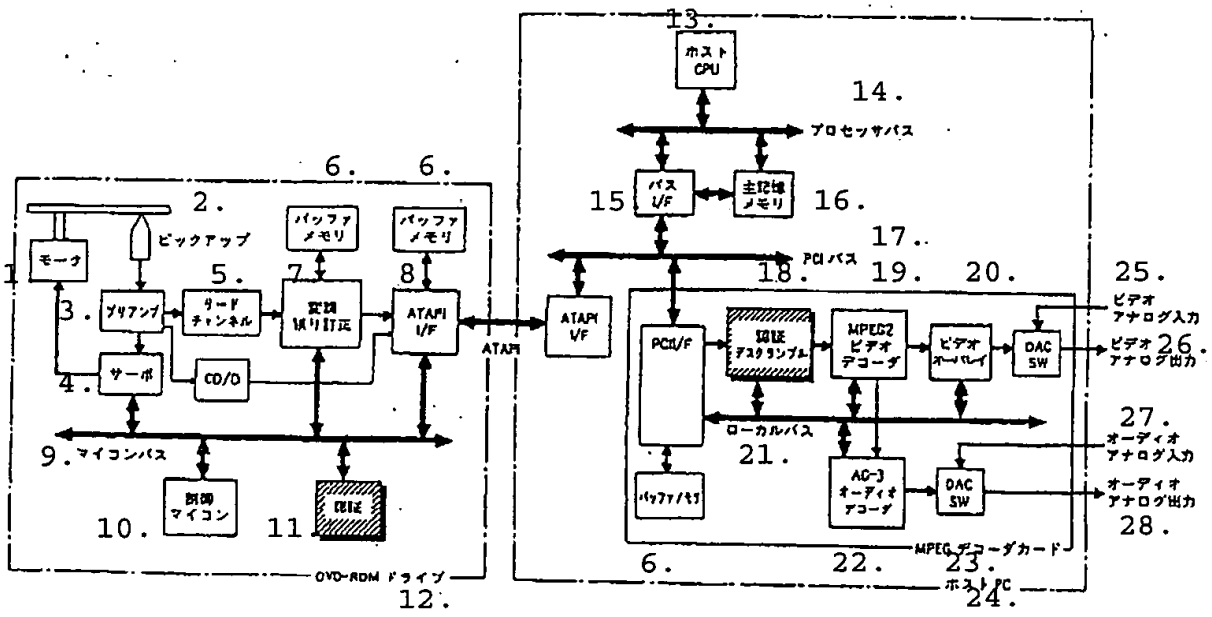


第5図 PCシステムにおけるバス認証とコンテンツ復号

Fig. 5 Bus-authentication and content descramble in PC system.

[(1): Encrypted disc key set; (2): Encrypted title key; (3): Scrambled AV data; (4): Bus authentication; (5): <DVD-ROM drive>; (6): Mutual authentication; (7): PC bus; (8): Bus authentication; (9): Master key; (10): Decoding; (11): Disc key; (12): Title key; (13): Descramble; (14): MPEG decoder; (15): <MPEG decoder module>]

Figure 6: Approximate constitutions of DVD-ROM drive and MPEG decoder module in a PC system



[(1): Motor; (2): Pickup; (3): Preamplifier; (4): Servo; (5): Lead channel; (6): Buffer memory; (7): Demodulation and error correction; (8): ATAPI I/F; (9): Microcomputer bus; (10): Controller microcomputer; (11): Authentication; (12): DVD-ROM drive; (13): Host CPU; (14): Processor bus; (15): Bus I/F; (16): Main memory; (17): PC bus; (18): Authentication and descramble; (19): MPEG2 video decoder; (20): Video overlay; (21): Local bus;

(22): AC-3 audio decoder; (23): MPEG decoder card; (24): Host PC; (25): Video analog input; (26): Video analog output; (27): Audio analog input; (28): Audio analog output]